Coleman-Gross and Mazur-Tate p-adic heights and integral points on hyperelliptic curves(Joint with J. Balakrishnan)

Amnon Besser

2012-04-25

Outline

Goal

- A new method for finding integral points on (certain) hyperelliptic curves $y^2 = Q(x)$.
- Gives an explicit function I on the p-adic points and a set of values T such that I takes a value in T on every integral point.
- Gives good bounds on the number of points.

Rational points on curves

- C - a smooth projective curve over $\mathbb{Q}$.
- Affine equation $f(x,y)=0$, $f \in \mathbb{Q}[x,y]$.
- Genus $g = g(C) =$ "Number of holes" in $\{(z,w) \in \mathbb{C}^2\ ,\ f(z,w)=0\}$.

Theorem (Faltings)

If $g \geq 2$, then $C(\mathbb{Q})$, the set of pairs (α,β) of rational numbers such that $f(\alpha,\beta)=0$, is finite

- Not effective

Chabauty's method

- In 1941 Chabauty proved finiteness of $C(\mathbb{Q})$ in some cases.
- His method was made effective, with really good bounds, by Coleman.
- Lots of numerical work using this method.

The Jacobian variety J of C

- J is an abelian variety, $J(F)$ is an abelian group for any field F.
- $J(F) =$ divisors of degree 0 on C, $\sum n_i(P_i)$ defined over F, modulo divisors of rational functions on C defined over F.
- If $P_0 \in C(\mathbb{Q})$ we have a map $C \to J$ given by $P \mapsto (P) - (P_0)$.
- J has dimension g, typically many equations in many variables.

The logarithm map

- $J(\mathbb{Q}_p)$ is a p-adic Lie group
- Its Lie algebra L has dimension g.
- There is a logarithm homomorphism $\log : J(\mathbb{Q}_p) \to L$
  - Near 0 it is an inverse to the exponential map
  - $\log(Q) = \log(nQ)/n$ with nQ near 0.

Chabauty's theorem

- Mordell-Weil implies $J(\mathbb{Q})$ is a finitely generated abelian group.
- Let $r = $ rank of $J(\mathbb{Q})$.

Theorem (Chabauty)

If $g > r$ then $C(\mathbb{Q})$ is finite.

Proof of Chabauty's theorem

- Let $Q_1, \ldots, Q_r$ be a basis of $J(\mathbb{Q})$.
- By dimensions $\exists$ a functional α on L vanishing on $\log(Q_1), \ldots, \log(Q_r)$.
- so $\alpha \circ \log$ vanishes on $J(\mathbb{Q})$.
- In particular, $\ell(P) := \alpha(\log((P) - (P_0)))$ vanishes on $C(\mathbb{Q})$.
- ℓ is locally analytic, hence has a finite number of zeros.

Coleman's contribution

- Coleman (1985) interpreted α as a holomorphic form ω on C and $\ell = \ell_\omega$ as the Coleman integral $\int_{P_0}^{P} \omega$.
- As a function of P it is a primitive of ω.

Theorem (Coleman)

If $p > 2g$ is a prime of good reduction and $r < g$, then the number of points in $C(\mathbb{Q})$ is at most $p + 1 + 2g\sqrt{p} + 2g - 2$

Kim's non-abelian Chabauty

- If $r \geq g$ Chabauty fails completely.
- Kim: Replace Coleman integrals with iterated Coleman integrals
  - e.g.,

$$\int(\omega \times \int \eta)$$

  - Each integral involves a choice of constant of integration.
  - Coleman integrals are locally analytic.
  - Computable in many cases (Balakrishnan, de Jeu and Escriva).
- J is replaced by a "Selmer variety".

Kim's Theorem

Theorem (Kim, + Balakrishnan, Kedlaya, Kim)

Let $E/\mathbb{Q}$ be an elliptic curve, in minimal model, with the following properties

- $r = 1$
- *p is a good reduction prime s.t. the p-part of the Tate-Shafarevich group of E is finite*
- *At each bad reduction prime the Néron model has just one component.*

Then, there exists an explicit Coleman integral τ on $E(\mathbb{Q}_p)$ such that $\tau(P)/(\int_0^P \omega)^2$ is constant on integral points, where ω is the invariant differential.

Hyperelliptic curve C

- Easy equation $y^2 = Q(x)$.
- More general (required for minimality)

$$y^2 + R(x)y = Q(x)\ ,\ 2\deg R \leq \deg Q$$

- $\deg Q = 2g + 1$
- Standard basis for $\Omega^1(C/\mathbb{Q})$

$$\{\omega_i,\ i = 0, \ldots, g-1\}, \omega_0 = \frac{dx}{2y + R(x)}\ , \omega_i = x^i \omega_0$$

- Standard dual basis $\bar{\omega}_i = (2i+1)x^{2g-1-i}\omega_0$

The main Theorem

Theorem (B. + Balakrishnan)

Let C be a hyperelliptic curve in minimal model. Suppose that Chabauty's method does not apply to C and that $r = g$. Then there exists constants $a_{ij} \in \mathbb{Q}_p$ and a finite set of values T such that

$$I(P) = \sum_{i=0}^{g-1} \int (\omega_i \times \int \bar{\omega}_i) + \sum_{ij} a_{ij} (\int_0^P \omega_i)(\int_0^P \omega_j)$$

obtains on each integral point of C a value in T.

- In particular, for an elliptic curve E one recovers Kim's result without the assumption on Tate-Shafarevich.

Classical height pairings on elliptic curves

- $E/\mathbb{Q}$ elliptic, $P = (x, y) \in E(\mathbb{Q})$
- $H(P) = H(x)$, $H(a/b)$ with a, b coprime is $\max(|a|, |b|)$.
- $h = \log(H)$ is quadratic up to a bounded function.
- Tate: Canonical height

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}$$

- $\hat{h}$ quadratic $\to \langle\ ,\ \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}$.

History

- Birch-Swinnerton-Dyer conjecture:

$$L^*(E,1) = \frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \prod c_p \cdot |\mathrm{Sha}(E)|}{|E(\mathbb{Q})_{\mathrm{tor}}|^2}$$

  where Reg_E is the determinant of the height pairing.
- Extend to Abelian varieties A over a number field F.
- Néron: decoposition into local heights $\hat{h} = \sum_{v \leq \infty} h_v$

History

- Bloch (1980): interpretation in terms of biextensions
- P. Schneider (1982): p-adic height pairing $h^p_\chi : A(F) \times A(F) \to \mathbb{Q}_p$ depending on $\chi = \prod \chi_v : I_F/F^\times \to \mathbb{Q}_p$, $h^p = \sum_{v<\infty} h^p_v$.
- Mazur Tate Teitelbaum (1986) p-adic BSD.
- Mazur Tate (1991) expressions for the p-adic height in terms of the p-adic σ function.
- Mazur Tate Stein - computation of p-adic height for elliptic curves.

History

- Gross (1985) Height pairings on Jacobians: h_v in terms of intersection theory, h_∞ by "Green functions"
- Coleman-Gross (1989) p-adic height pairings on jacobians: h_v for $v|p$ by Coleman integration theory.
- (B + Balakrishnan) Implementation of Coleman-Gross for hyperelliptic curves.

p-adic height pairings on curves - Coleman Gross (1985)

- Needs the following data
  - C/F smooth complete curve, good reduction above p.
  - $\chi : I_F/F^\times \to \mathbb{Q}_p$ as in Schneider
  - A choice, for each $v|p$ of a complementary subspace W to F^0 in $H^1_{\mathrm{dR}}(C_v/F_v)$.
- $x, y \in Div_0(C_v)$ with disjoint supports give $h_v(x, y) \in \mathbb{Q}_p$, symmetric bilinear s.t., $h_v((f), y) = \chi_v(f(y))$ for a rational function f.

Local height h_v for v not dividing p

- $\tilde{C}$ regular model for C_v
- $\tilde{y}, \tilde{z}$ extensions of y and z to rational

divisors on $\tilde{C}$, one of which has zero intersection with special fiber.

$$h_v(y, z) = \tilde{y} \cdot \tilde{z} \cdot \chi_v(\pi_v)$$

Local height h_v for $v|p$

Can be defined using the p-adic Green function

$$h_v(\sum n_i(x_i), \sum m_j(y_j)) = \mathrm{tr}_v(G((\sum n_i(x_i), \sum m_j(y_j)))$$

$$G(\sum n_i(x_i), \sum m_j(y_j)) = \sum_{ij} n_i m_j G(x_i, y_j)$$

Heights for non-disjoint supports

- Gross, based on ideas of Tate
- Additional choice: Tangent vectors $\{t_P \ , \ P \in C\}$.
- Local pairings should now satisfy
  - $h_v((f), y) = \chi_v(f[y])$ where $f[y]$ is a normalized value.
  - Change of vector formula: $t_P \to \alpha t_P$ adds $\chi_v(\alpha) \deg_P(x) \deg_P(y)$
- Formulas when v does not divide p: Same, with $\tilde{P} \cdot \tilde{P} = 0$ provided t_P is a generator of tangent bundle at $\tilde{P}$.
- Formulas when $v|p$: same with $G(P, P)$ interpreted as the "constant term" of $G(P, \cdot)$ at P with respect to t_P

The main technical result

- C given by $y^2 = f(x)$ over $\mathbb{Q}_p$.
- t_x is dual to $dx/2y$ at all points except the point at infinity, dual to $x^{g-1}dx/y$ at that point.
- Define

$$\tau = -2\sum_{i=0}^{g-1}\int\left(\omega_i \times \int \bar{\omega}_i\right)$$

Theorem ((B+Balakrishnan))

With the above choice of tangent vectors we have

$$G((x)-(0),(x)-(0)) = \tau(x)$$

The proof uses p-adic Arakelov theory.

Proof of the main theorem

- Either Chabauty's method applies, or the functionals $\psi_i = \alpha_{\omega_i} \circ \log$ form a basis to $\mathrm{Hom}(J(\mathbb{Q}), \mathbb{Q}_p)$.
- $\psi_i \cdot \psi_j$ form a basis to the vector space of $\mathbb{Q}_p$ valued quadratic forms on $J(\mathbb{Q})$.
- h is also quadratic, so we have a_{ij} with $h + \sum a_{ij}\psi_i \cdot \psi_j = 0$
- For $P \in C(\mathbb{Q})$ this means $h((P) - (0), (P) - (0)) + \sum a_{ij} \int_0^P \omega_i \int_0^P \omega_j = 0.$
- $h((P) - (0), (P) - (0)) - \tau(P) = \sum_{q \neq p} h_q((P) - (0), (P) - (0)).$
- If C has good reduction at q, $h_v = 0$ by integrality.
- Otherwise, depends on which component of special fiber P hits.